Aula 09

OS TEOREMAS DE SYLOW

META

Estabelecer os teoremas de Sylow.

OBJETIVOS

Identificar $p - SS$.

Aplicar os teoremas de Sylow na resolução de problemas.

PRÉ-REQUISITOS

O curso de Fundamentos de Matemática e as aulas anteriores.

INTRODUÇÃO

Esta é a última aula deste curso sobre a Teoria dos grupos. Vamos estabelecer os teoremas de Sylow que, após os teoremas de Lagrange e Cauchy, constituem os primeiros resultados importantes decorrentes das propriedades aritméticas das ordens dos grupos finitos.

Nesta aula, iniciaremos estabelecendo o conceito de ação de grupos sobre conjuntos de modo sucinto, definindo e apresentando apenas os propriedades que utilizaremos nas demonstrações dos três teoremas de Sylow que são os resultados importantes desta aula.

AÇÃO DE GRUPOS EM CONJUNTOS

Definição 1. Sejam G um grupo e X um conjunto não vazio. Chamamos ação de G em X a qualquer aplicação de G x $X \longrightarrow X$, que escrevemos, G x $G \longrightarrow a * x$, satisfazendo às seguintes propriedades:

i) $\forall x \in X, e * x = x$

ii) $\forall a, b \in G, a * (b * x) = (ab) * x$

Exemplo 1. Seja G um grupo para $X = G$, a aplicação de G x $G \longrightarrow G$ dada por $a * x = ax$ é uma ação de G em si próprio.

Exemplo 2. Sejam $H \trianglelefteq G$ e $X = \frac{G}{H}$.

Então, a aplicação G x $\frac{G}{H} \longrightarrow H$ dada por $a * bH = abH$ é uma ação no conjunto quociente ${}^{G}/_{H}$.

Observação. Quando o grupo G age no conjunto X, para cada $a \in G$. Define-se uma transformação $T_a : X \longrightarrow X$ onde $T_a(x) = a * x$.

É fácil ver que cada T_a é bijetiva onde $(T_a)^{-1} : X \longrightarrow X$ é dada por $(T_a)^{-1}(y) = a^{-1} * y$.

A ação de um grupo G nem conjunto X, define uma relação de equivalência neste, assim definida: $xRy \Leftrightarrow \exists a \in G$ tal que $y = a * x$.

Notemos que $x = e * x \quad \forall x \in X$, se em X, xRy então existe $a \in G$ tal que $y = a * x$ donde temos que $x = a^{-1} * y$ e, yRx. Se $x, y, z \in X$ tais que xRy e yRz então existem $a, b \in G$ tais que $y = a * x$ e $z = b * y$, donde temos que $z = b * (a * x) = (ba) * x$ logo, aRz.

Dados G grupo e X conjunto com G agindo em X, definimos a G-órbita do elemento $x \in X$, como sendo a classe de equivalência de x e a indicamos por $O(x)$

Precisamente, $\mathcal{O}(x) = \{a * x; a \in G\}$. Indicamos o conjunto quociente (das órbitas) por ${}^{X}/_{G}$.

Quando X é finito, lembremos que existem $x_1, x_2, \dots, x_n \in X$ tais que $X = \biguplus \mathcal{O}(x_i)$ e $|G| = \sum_{i=1}^{n} |\mathcal{O}(x_i)|$.

Definição 2. Dados G grupo, X conjunto com G agindo em X e, $x \in X$, definimos o estabilizador (ou subgrupo de isotropia) de x, como sendo o conjunto

$$G_x = \{a \in G; a * x = x\}.$$

Notemos que $e * x = x \Longrightarrow e \in G_x$. Se $a, b \in G_x$ então $a * x = x$ e $b * x = x \Longrightarrow b^{-1} * x = x$ e $(ab^{-1}) * x = a * (\mathrm{b}^{-1} * x) = a * x = x \Longrightarrow ab^{-1} \in G_x$. Portanto, para cada $x \in X$, o estabilizador de x é um subgrupo de G, como já informamos na definição, chamado também de subgrupo de isotropia do elemento x de X.

Notemos também que se $x, y \in X$ estão na mesma órbita, isto é, $\mathcal{O}_x = \mathcal{O}_y$ então, seus estabilizadores são conjugados, pois se $y = a * x$, para algum $a \in G$, temos:

$b \in G_x \Leftrightarrow b * x = x \Leftrightarrow b * (a^{-1} * y) = a^{-1} * y \Leftrightarrow (ba^{-1}) * y = a^{-1} * y \Leftrightarrow a * \left((ba^{-1}) * y\right) = y \Leftrightarrow (aba^{-1}) * y = y \Leftrightarrow aba^{-1} \in G_y \Leftrightarrow G_y = a^{-1} G_x a = G_x^a$. Portanto, G_x e G_y são conjugados.

Proposição 1. Sejam G um grupo e X um conjunto com G agindo em X então, para cada $x \in X, |\mathcal{O}_x| = [G : G_x]$.

Demonstração. Consideramos para cada $x \in X$, a aplicação $\psi : \mathcal{O}_x \longrightarrow {}^{G}/_{G_x}$ dada por $\psi(a) = aG_x$. Então, para $a, b \in \mathcal{O}_x$, $\psi(a) = \psi(b) \Leftrightarrow aG_x = bG_x \Leftrightarrow b^{-1}a \in G_x \Leftrightarrow (b^{-1}a) * x = x \Leftrightarrow a * x = b * x$. Logo, ψ é injetiva. Como estamos lidando com conjuntos finitos, temos a bijetividade. Portanto, $|\mathcal{O}_x| = [G : G_x]$.(ou $|G| = |\mathcal{O}_x|.|G_x|$).

Observação. Para $\frac{G}{X} = \{\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_n}\}$, temos $|X| = \sum_{i=1}^{n} \left|\mathcal{O}_{x_i}\right| = \sum_{i=1}^{n} [G : G_{x_i}]$

OS TEOREMAS DE SYLOW

Proposição 1. (1º teorema de Sylow). Sejam G um grupo finito e $p \in \mathbb{Z}_+$ um primo onde $|G| = p^n.m$, onde $m, n \in \mathbb{N}$. Então G possui um subgrupo H de G de ordem p^n.

Demonstração. Seja $X = \{S | S \subseteq G$ e $|G| = p^n\}$ o conjunto de todos os subconjuntos de G com p^n elementos.

Façamos G agir em X do seguinte modo: $\forall a \in G$ e $\forall S \in X$, $a * S = aS = \{as; s \in S\}$.

Notemos que $|aS| = |S|$ ($\Longrightarrow aS \in X$).

$$|X| = \binom{p^n m}{p_n} = \frac{(p^n m)!}{p^n!(p^n m - p^n)!} = \frac{p^n m(p^n m-1).....(p^n m - p^n + 1)}{p^n(p^n - 1)\ .....\ 2.1}$$

Notemos que para $0 \leq k \leq n$ e $1 \leq i \leq p^n$, $p^k | p^n m - i \Leftrightarrow p^k | i \Leftrightarrow p^k | p^n - i$. Logo, $p^r \Big| |X| \Leftrightarrow p^r | m$.

Seja p^r a potência de p de maior expoente na fatoração em primos de $|X|$ (ou de m). Como $|X| = \sum_{S \in X} |\mathcal{O}_S|$, $p^r \Big| |X|$ e $p^{r+1} \nmid |X|$, existe pelo menos uma destas órbitas, digamos $\{S_1, S_2, \dots, S_k\}$ tal que $p^{r+1} \nmid k$.

Seja S_i um elemento desta órbita, então $|G| = |\mathcal{O}_{S_i}|.|G_{S_i}| \Rightarrow p^n m = k.|G_{S_i}|$

Como $p^r | m$ e $p^{r+1} \nmid m$ temos que $p^{n+r} \Big| k.|G_{S_i}|$. Lembrando que $p^{r+1} \nmid k \Rightarrow p^n \Big| |G_{S_i}| \Rightarrow |G_{S_i}| \geq p^n$.

Finalmente, como $G_{S_i} = \{a \in G; aS_i = S_i\}$ temos que $\forall s \in S_i$, $G_{s_i} s \subseteq S_i$, além disto, $|G_{s_i} s| = |G_{s_i}|$, logo $|G_{s_i}| \leq |S_i| = p^n$.

As duas desigualdades acima implicam que $|G_{S_i}| = p^n$ e portanto, existe $H = G_{S_i} \leq G$ tal que $|H| = p^n$.

Observação: O teorema de Cauchy é um caso especial deste teorema.

Sejam, G um grupo finito, $p \in \mathbb{N}$ um primo e $H \leq G$.

Definição 1. Dizemos que H é um p-subgrupo de Sylow de G se $|H|$ é a potência de p, de maior expoente, que divide a ordem de G.

Ou seja H é um $p - SS$ se $|G| = p^n.m$ com $m, n \in \mathbb{N}$ e $p \nmid m$.

Proposição 2. (2º teorema de Sylow). Sejam G um grupo finito e $p \in \mathbb{N}$ um primo divisor da ordem de G. Então, todos os $p - SS$ são conjugados. Ou seja, se $H, L \leq G$ são p-subgrupos de Sylow, então existe $a \in G$ tal que $L = a^{-1}Ha$.

Demonstração. Seja H um $p - SS$ de G. Então $|G| = p^n m$ com $m, n \in \mathbb{N}, p \nmid m$ e $|H| = p^n$. Temos então que $[G : H] = m$.

Seja $X = \{aH; a \in G\}, (\Rightarrow |X| = m)$ e seja K um outro $p - SS$ de G. Façamos K agir em X pela regra $g * aH = gaH$.

Como $|X| = m = \sum_{aH \in X} |\mathcal{O}_{aH}|$ e $p \nmid m$, existe uma órbita $\mathcal{O}_{a_1 H}$ com k elementos tal que $p \nmid k$. Seja $a_1 H$ um elemento desta órbita. Então, o estabilizador deste elemento é $K_{a_1 H} = \{a \in K; aa_1 H = a_1 H\} = \{a \in K; a_1^{-1} a\, a_1.H = H\} = \{a \in K; a_1^{-1} a a_1 \in H\} = \{a \in K; a \in a_1 H a_1^{-1}\}$.

Ou seja $K_{a_1 H} = H \cap a_1 H a_1^{-1}$.

Como $|K| = |K_{a_1H}|.|\mathcal{O}_{a_1H}|$ temos que $p^n = |K \cap a_1Ha_1^{-1}|.k$. Como $p \nmid k$ segue que $k = 1$ e $|K \cap a_1H| = p^n$. Conseqüentemente $K \cap a_1Ha_1^{-1} = K = a_1H\, a_1^{-1}$ e portanto, H e K são conjugados.

Proposição 3. (3º teorema de Sylow). Sejam G um grupo finito e $p \in \mathbb{N}$ um primo divisor da ordem de G. Então, o número de $p - SS$ de G é um divisor do índice comum destes subgrupos e, é congruente a 1 módulo p.

Demonstração. Sejam $|G| = p^n.m$ com $m.n \in \mathbb{N}$ e $p \nmid m$. Seja r_p o número de $p - SS$ de G. Devemos mostrar que $r_p|m$ e que $r_p \equiv 1(mod\, p)$. Com efeito, sejam H um $p - SS$ de G, $X = \frac{G}{H} = \{aH; a \in G\}$ e a ação de G em X definida por $g * aH = gaH$. Notemos que dados $aH, bH \in X$, existe $ba^{-1} \in G$ tal que $bH = ba^{-1} * aH$ donde temos que $\mathcal{O}_{aH} = \mathcal{O}_{bH}$, ou seja, para esta ação temos apenas uma órbita ($\Longrightarrow$ Todos os grupos de isotropia dos elementos de X são conjugados ($\Longrightarrow$ têm a mesma ordem)).

Seja aH um elemento pré-fixado de X. Então $G_{aH} = \{g \in G; gaH = aH\} = \{g \in G; a^{-1}gaH = H\} = \{g \in G; g \in aHa^{-1}\} = aHa^{-1}$. Ou seja, o estabilizador de aH é o $p - SS$ aHa^{-1}.

Sejam $a_1H, \dots, a_rH$ os elementos de X que tem H como estabilizador. Então, para $i \in \{1, \dots, r\}, ha_iH = a_iH\ \forall h \in H \Leftrightarrow a_i^{-1}ha_iH = H\ \forall h \in H \Leftrightarrow a_i^{-1}ha_i \in H, \forall h \in H \Leftrightarrow$
$Ha_i = a_iH$.

Agora notemos que para cada $i \in \{1, \dots, r\}$, e para cada $h \in H,\ aha^{-1}.aa_iH = aha_iH = ahHa_i = aHa_i = aa_iH$. Segue que os elementos $aa_iH, \dots, aa_rH$ são estabilizados pelo $p - SS$ $aHa^{-1} = \{aha^{-1}; h \in H\}$.

Sejam $a_iH, \dots, a_sH$ os elementos de X que são estabilizados por aHa^{-1}. Então, para cada $j \in \{1, \dots, s\}$ e cada $h \in H$, temos $aha^{-1}.a_jH = a_jH \Longrightarrow h.a^{-1}a.H = a^{-1}a_jH$ segue que $a^{-1}a_jH$ é estabilizado por H. Temos então que $r \leq s$ e $s \leq r$ ou seja $r = s$.

Logo, cada $p - SS$ de G estabiliza o mesmo número de elementos de X.

Como $|X| = m + r.r_p$ temos que $r_p|m$ como queríamos.

Agora, façamos o $p - SS$ H de G agir em $X = \{aH; a \in G\}$ pela ação $h * aH = haH$ (mesma lei de definição de antes). Sabemos que para cada $aH \in X$, $|\mathcal{O}_{aH}|\,|p^n$ donde segue que o número de elementos de cada órbita é 1 ou uma potência de p. Se $|\mathcal{O}_{aH}| = 1$ então $\mathcal{O}_{aH} = \{aH\} \Leftrightarrow \{haH; h \in H\} = \{aH\} \Leftrightarrow haH = ah\ \forall h \in H \Leftrightarrow G_{aH} = H$. Isto implica que existem r órbitas, sob a ação de H com um único elemento. Como as ordens não unitárias são múltiplos de p, existe $u \in \mathbb{N}$ tal que $|X| = m = r + u.p$ ou seja, $m \equiv r(mod\, p)$ como, $m = r.r_p$, temos $r.r_p \equiv r(mod\, p) \Longrightarrow p|r(r_p - 1)$ e como $p \nmid m\ (\Longrightarrow p \nmid r)$ ou seja $p|r_p - 1$ e portanto $r_p \equiv 1(mod\, p)$. Como queríamos demonstrar.

Exemplo 1. Seja G, um grupo de ordem 15. Vamos provar que G tem um subgrupo normal. De fato, seja n_5 o número de subgrupos de G de ordem 5. Pelo 3º teorema de Sylow, temos que $n_5 \equiv 1(mod\ 5)$ e $n_5|3$. Segue que $n_5 = 1$. Como existe um único 5-subgrupo de Sylow, pelo 2º teorema de Sylow este subgrupo é normal.

RESUMO

Estabelecemos inicialmente a ação de um grupo num conjunto, apresentado suas propriedades onde preparamos os pré-requisitos para as demonstrações dos teoremas de Sylow. Apresentamos os teoremas, definimos os $p - SS$, demonstramos os teoremas e terminamos com um exemplo no qual aplicamos o 3º e 2º teoremas de Sylow.

ATIVIDADES

1. Seja G um grupo de ordem 24. Prove que G tem um subgrupo H tal que $|H| = 4$.

2. Seja G um grupo de ordem pq onde p e q são primos positivos tais que $p < q$. Prove que G tem um subgrupo H normal de ordem q.

3. Se G é simples e abeliano, prove que $|G|$ é um número primo.

4. Suponhamos que G é um grupo simples cuja ordem é $p^n.m$ onde $m, n \in \{2,3, \dots\}$ e $p \in \mathbb{Z}_+$ é primo e $p \nmid m$. Prove que G tem no mínimo dois $p - SS$.

COMENTÁRIO DAS ATIVIDADES

Caro aluno, você deve ter notado que para fazer a primeira atividade basta aplicar diretamente o primeiro teorema de Sylow.

Na segunda, você deve ter imitado o exemplo 3.

A terceira atividade, se você conseguiu fazê-la, você deve ter usado o fato de que todo subgrupo de um grupo abeliano é normal.

Na quarta atividade, usando o 2º teorema de Sylow, se G tivesse apenas um $p - SS$, este seria normal.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).